CIPHERING DEVICE AND DECIPHERING DEVICE

Patent Number: JP2002190798
Publication date: 2002-07-05
Inventor(s): NINO YUICHI; NAKAMURA NOBUTATSU
Applicant(s): NEC CORP
Requested Patent: JP2002190798
Application Number: JP20000386556 20001220
Priority Number(s):
IPC Classification: H04L9/16
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To obtain ciphering and deciphering devices capable of reducing the load of ciphering and deciphering processing for various data and applying strong ciphering processing to important data.
SOLUTION: Original data to be the source of data to be transmitted are divided by a data block division means 242 in each sort of data on the basis of an analytical rule 241 stored in an analytical rule storing part 224. Then a data block ciphering means 244 ciphers each data block in accordance with importance on the basis of the contents of the analytical rule 241 to prepare a ciphered data block. A data block integration means 245 integrates the ciphering method of each ciphered data block and the positional information of a storage area storing the ciphered data block as ciphered data and sends the ciphered data to a client. Since ciphering strength can be changed in accordance with the soft of data constituting the original data, efficient ciphering and deciphering processing can be performed and the load of the ciphering device and the deciphering device can be reduced.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－190798
(P2002－190798A)
(43)公開日　平成14年７月５日(2002.7.5)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/16		Ｈ０４Ｌ　9/00	６４３	５Ｊ１０４

審査請求　未請求　請求項の数６　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－386556(P2000－386556)

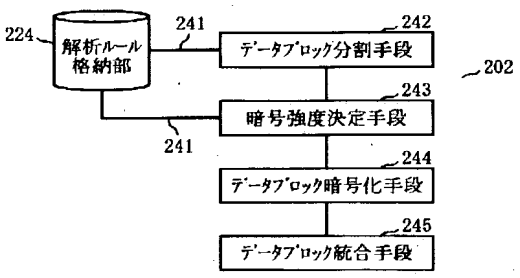
(22)出願日　平成12年12月20日(2000.12.20)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　仁野　裕一
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　中村　暢達
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100083987
弁理士　山内　梅雄

Ｆターム(参考)　5J104 AA01 AA37 AA38 DA04 JA03 NA02 PA07

(54)【発明の名称】　暗号化装置および復号化装置

(57)【要約】
【課題】　各種データに対して暗号化および復号化の処理の負担を軽減することができると共に重要なデータに対して強度の暗号化処理が可能な暗号化装置および復号化装置を得ること。
【解決手段】　送信するデータの元となる原データは解析ルール格納部２２４に格納された解析ルール２４１によって、まずデータの種類別にデータブロック分割手段２４２で分割される。そして解析ルール２４１の内容に沿って重要度に応じて、データブロック単位でデータブロック暗号化手段２４４が暗号化を行い暗号化データブロックを作成する。データブロック統合手段２４５は暗号化データブロックのそれぞれの暗号化方法と、暗号化データブロックの格納されている記憶領域の位置情報とを暗号化データとして統合し、クライアント側に送出する。原データを構成するデータの種類に応じて暗号化の強度を変えることができるので、効率的な暗号化処理および復号を行うことができ、暗号化装置および復号化装置の負担を軽減できる。



1

【特許請求の範囲】

【請求項１】　送信すべき原データの重要度をその原データの各部分について判別する重要度判別手段と、
この重要度判別手段によって判別した重要度に応じて原データのそれぞれの部分の暗号化の強度を選択する暗号化強度選択手段と、
この暗号化強度選択手段によって選択された強度で原データのそれぞれ該当する部分を暗号化する原データ暗号化手段とを具備することを特徴とする暗号化装置。

【請求項２】　送信すべき原データを構成する各部のデータの種類を判別する種類判別手段と、
この種類判別手段によって判別された種類ごとに原データをデータブロックに分割する原データ分割手段と、
この原データ分割手段によって分割された各データブロックについてこれらを構成するデータの種類を基にして暗号化の強度の重要度を判別する重要度判別手段と、
この重要度判別手段によって判別した重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択する暗号化強度選択手段と、
この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを具備することを特徴とする暗号化装置。

【請求項３】　送信すべき原データを構成する各部のデータの種類を判別する種類判別手段と、
この種類判別手段によって判別された種類ごとに原データをデータブロックに分割する原データ分割手段と、
この原データ分割手段によって分割された各データブロックの長さを判別するブロック長判別手段と、
このブロック長判別手段によって判別されたブロック長およびデータブロックごとのデータの種類を基にして暗号化の強度の重要度を判別する重要度判別手段と、
この重要度判別手段によって判別した重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択する暗号化強度選択手段と、
この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを具備することを特徴とする暗号化装置。

【請求項４】　送信すべき原データを構成する各部のデータの種類を判別する種類判別手段と、
この種類判別手段によって判別された種類ごとに原データをデータブロックに分割する原データ分割手段と、
前記原データ分割手段によって分割されたデータブロックの種類ごとに復号が行われる側での復号の予定時間を検出する復号予定時間検出手段と、
この復号予定時間検出手段によって検出された時間に合わせて暗号化の強度を選択する暗号化強度選択手段と、
この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを具備することを特徴とする暗号化装置。

【請求項５】　暗号化されたデータを受信してこれをデータの種類別のデータブロックに分割するデータブロック分割手段と、
このデータブロック分割手段で分割したそれぞれのデータブロックを前記暗号化されたデータの受信の際に受信されたデータブロックごとの暗号化方法を示すデータを基にしてデータブロック単位に復号するデータブロック復号手段と、
このデータブロック復号手段によって復号された各データブロックを統合して暗号化する前の原データを再現するデータ統合手段とを具備することを特徴とする復号化装置。

【請求項６】　前記データブロック復号手段は、データブロックごとの暗号化方法を示すデータが暗号化されているか否かを判別する暗号化有無判別手段と、この暗号化有無判別手段が暗号化されていると判別したとき予め取得した暗号鍵を使用して前記データブロックごとの暗号化方法を復号する暗号化方法復号手段を備え、暗号化方法復号手段によって復号された暗号化方法を使用して対応するデータブロックの復号を行うことを特徴とする請求項５記載の復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は暗号化装置および復号化装置に係わり、特に暗号化あるいは復号化の負担を軽減することのできる暗号化装置および復号化装置に関する。

【０００２】

【従来の技術】インターネットに代表される通信ネットワークが広く利用されるようになってきている。またこのような通信ネットワークを使用して通信を行う通信機器として各種のものが登場している。これに伴って、各種のデータがこれらの通信機器によって送受信されるようになっている。たとえばインターネットおよび携帯型電話機に代表される情報通信端末の発展によって、音楽データ等の各種のデータを格納した種々のサーバから各種の情報通信端末にデータをダウンロードする機会が増えている。

【０００３】これらのサーバの中には前記した音楽データを配信するサーバや、特別に編集された経済情報を会員に配布するサーバのように配布するデータが特定の通信先に限定されているものがある。たとえば有料で音楽データを配布するような場合には、料金を支払う特定の通信先の情報通信端末に限定してデータを送出する必要がある。そこで、このようなデータは暗号化して情報通信端末に送信することで、他の情報通信端末がこれを受信して不当に解読を行わないようにすることが多い。

【０００４】ところが、特に携帯型電話機やＰＤＡ（personal digital assistants：個人向け携帯型情報通信機器）に代表される情報通信端末は通常のパーソナルコンピュータと比較すると搭載するハードウェアの制限等

によって信号の処理能力が低い場合が多い。このため、送出するデータに対して高度な暗号化を行うと、受信した情報通信端末側での復号化のための演算処理に手間取ったり過負荷がかかり他の処理に影響を与えるという不具合が発生するおそれがある。

【０００５】そこで、このような問題を解決するための提案が行われている。特開平７－２８１５９６号公報に示される第１の提案では、各データ・セグメントについて、複数個の暗号化関数の１つを選択し、選択した暗号化関数を使用してデータ・セグメントを暗号化して、暗号化データ・セグメントを形成している。そして、暗号化データ・セグメントを含む暗号化データ・ブロックを作成し、暗号化データ・ブロックに関して、データを暗号化するために使用された暗号化関数の指示を有する関連した制御ブロックを作成している。

【０００６】図１７は、特開平７－２８１５９６号公報に示される第１の提案の概要を示したものである。この提案では同図（ａ）に示すように、送信しようとするデータ１０１を複数個のデータブロック102_1～102_nに分割する。そして、それぞれのデータブロック102_1～102_nに対して順次異なった種類の暗号化を施し、同図（ｂ）に示すように暗号化されたデータブロック103_1～103_nの前に暗号化情報104_1～104_nを配置して、送信を行うようにしている。

【０００７】一方、特開平２０００－４７５８０号公報記載の第２の提案では、簡単な変換を繰り返し行うことで、複雑な暗号変換を構成する従来の手法に代えて、送信側のサーバと受信側の情報通信端末が異なった複数の暗号アルゴリズムで暗号化あるいは復号化を行う手段を用意している。データの送信を行う前に送信側のサーバと受信側の情報通信端末は、アルゴリズム情報と共通鍵をＰＫＩ（Public KeyInfrastructure：認証局サービス）等によって、互いに交換し、その交換された情報に基づいて暗号化したデータをサーバ側から送信し、受信側の情報通信端末で復号化するようにしている。

【０００８】これら２つの提案に共通している点は、受信側の情報通信端末が過負荷とならないように、従来と比較すると簡単に復号化できるような簡単なアルゴリズムを使用していることである。そして、他の情報通信端末が暗号アルゴリズムや暗号鍵の推定を容易に行えないようにするために、データの各構成部分あるいは各通信単位でこれら暗号アルゴリズムや暗号鍵を異なるものにしていることも共通している。

【０００９】

【発明が解決しようとする課題】このような提案を採用することによって、受信側の情報通信端末における暗号の解読の負担が多少軽減されることになる。しかし、このような手法を採ると、全てのデータブロックに対して、強度の弱い暗号化方法を採用してしまうこととなるので、データの中でも特に重要な部分が偶然復号化されてしまう恐れがある。一方で、インターネットで送受信するデータは全て重要であるケースはまれで、特定の重要部分が復号されなければ、他の部分が復号されても、データ送信者にとって不都合とならない場合が多い。例えば、画像データを配信する場合、画像サイズの１ピクセルあたりのデータ長、カラーマップなどを記載したヘッダが復号化されなければ、各画素のデータが仮に復号化されたとしてもクラッカは画像の内容を復元することはできない。

【００１０】そこで本発明の目的は、復号化の際の処理の負担を軽減でき、なおかつデータ送信者にとって復号されると不都合な重要なデータについては、強度の暗号化処理を行うことのできる暗号化および復号化装置を提供することにある。

【００１１】

【課題を解決するための手段】請求項１記載の発明では、（イ）送信すべき原データの重要度をその原データの各部分について判別する重要度判別手段と、（ロ）この重要度判別手段によって判別した重要度に応じて原データのそれぞれの部分の暗号化の強度を選択する暗号化強度選択手段と、（ハ）この暗号化強度選択手段によって選択された強度で原データのそれぞれ該当する部分を暗号化する原データ暗号化手段とを暗号化装置に具備させる。

【００１２】すなわち請求項１記載の発明では、送信すべき原データの重要度をその原データの各部分について判別し、判別した重要度に応じて原データのそれぞれの部分の暗号化の強度を選択するようにしている。そして、これら選択された強度で原データのそれぞれ該当する部分を暗号化することにしているので、重要度の高い部分は充分な強度で暗号化を行うことができる反面、これ以外の一般部分については暗号化の強度を弱くすることができるので、原データの全体に対して画一的に暗号化を強化した場合と比べて全体的な復号化の負担を軽減することができる。

【００１３】請求項２記載の発明では、（イ）送信すべき原データを構成する各部のデータの種類を判別する種類判別手段と、（ロ）この種類判別手段によって判別された種類ごとに原データをデータブロックに分割する原データ分割手段と、（ハ）この原データ分割手段によって分割された各データブロックについてこれらを構成するデータの種類を基にして暗号化の強度の重要度を判別する重要度判別手段と、（ニ）この重要度判別手段によって判別した重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択する暗号化強度選択手段と、（ホ）この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを暗号化装置に具備させる。

【００１４】すなわち請求項２記載の発明では、送信すべき原データを構成する各部のデータの種類を判別し

て、これら種類に応じて原データをデータブロックに分割するようにしている。そして、分割された各データブロックについてこれらを構成するデータの種類を基にして暗号化の強度の重要度を判別し、判別された重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択し、暗号化を行うようにしている。したがって、原データを構成するデータの種類に応じた強度で暗号化を行うことができ、きめ細かにかつ合理的に暗号化を行うことができるので、復号の際の処理の負担を軽減させることができる。

【００１５】請求項３記載の発明では、（イ）送信すべき原データを構成する各部のデータの種類を判別する種類判別手段と、（ロ）この種類判別手段によって判別された種類ごとに原データをデータブロックに分割する原データ分割手段と、（ハ）この原データ分割手段によって分割された各データブロックの長さを判別するブロック長判別手段と、（ニ）このブロック長判別手段によって判別されたブロック長およびデータブロックごとのデータの種類を基にして暗号化の強度の重要度を判別する重要度判別手段と、（ホ）この重要度判別手段によって判別した重要度に応じてそれぞれのデータブロックについての暗号化の強度を選択する暗号化強度選択手段と、（ヘ）この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを暗号化装置に具備させる。

【００１６】すなわち請求項３記載の発明では、送信すべき原データを構成する各部のデータの種類を判別して、これら種類に応じて原データをデータブロックに分割するようにしている。そして、分割された各データブロックごとにこれらを構成するデータの種類およびデータブロックの長さに応じた暗号化の強度を選択し、暗号化を行うようにしている。したがって、データブロックの長短を考慮した合理的な暗号化を行うことができ、復号の際の処理の負担を軽減させることができる。

【００１７】請求項４記載の発明では、（イ）送信すべき原データを構成する各部のデータの種類を判別する種類判別手段と、（ロ）この種類判別手段によって判別された種類ごとに原データをデータブロックに分割する原データ分割手段と、（ハ）原データ分割手段によって分割されたデータブロックの種類ごとに復号が行われる側での復号の予定時間を検出する復号予定時間検出手段と、（ニ）この復号予定時間検出手段によって検出された時間に合わせて暗号化の強度を選択する暗号化強度選択手段と、（ホ）この暗号化強度選択手段によって選択された強度でデータブロックごとに暗号化を行う暗号化手段とを暗号化装置に具備させる。

【００１８】すなわち請求項４記載の発明では、送信すべき原データを構成する各部のデータの種類を判別して、これら種類に応じて原データをデータブロックに分割するようにしている。そして、分割されたデータブロックの種類ごとに復号が行われる側での復号の予定時間を検出し、検出された時間に合わせてデータの種類も考慮しながら暗号化の強度を選択するようにしている。したがって、暗号化されたデータを復号する装置側の負荷等を考慮しながら合理的な暗号化を行うことができ、復号の際の処理の負担を軽減させることができる。

【００１９】請求項５記載の発明では、（イ）暗号化されたデータを受信してこれをデータの種類別のデータブロックに分割するデータブロック分割手段と、（ロ）このデータブロック分割手段で分割したそれぞれのデータブロックを暗号化されたデータの受信の際に受信されたデータブロックごとの暗号化方法を示すデータを基にしてデータブロック単位に復号するデータブロック復号手段と、（ハ）このデータブロック復号手段によって復号された各データブロックを統合して暗号化する前の原データを再現するデータ統合手段とを復号化装置に具備させる。

【００２０】すなわち請求項５記載の発明では、請求項１～請求項４に記載した暗号化装置で暗号化されたデータを復号する復号化装置を扱っている。すなわち、データブロック分割手段は暗号化されたデータを受信してこれをデータの種類別のデータブロックに分割し、データブロック復号手段はそれぞれのデータブロックごとの暗号化方法を示すデータを基にしてデータブロック単位に復号を行う。データ統合手段は復号されたデータブロックを統合して暗号化する前の原データを再現するようにしている。

【００２１】請求項６記載の発明では、請求項５記載の復号化装置で、データブロック復号手段は、データブロックごとの暗号化方法を示すデータが暗号化されているか否かを判別する暗号化有無判別手段と、この暗号化有無判別手段が暗号化されていると判別したとき予め取得した暗号鍵を使用してデータブロックごとの暗号化方法を復号する暗号化方法復号手段を備え、暗号化方法復号手段によって復号された暗号化方法を使用して対応するデータブロックの復号を行うことを特徴としている。

【００２２】すなわち請求項６記載の発明では、データブロックごとの暗号化方法を暗号化して復号化装置側に送ってきた場合には、予め通信等で取得した暗号鍵を使用してデータブロックごとの暗号化方法を復号し、これを用いて対応するデータブロックの復号を行うことにしている。

【００２３】

【発明の実施の形態】

【００２４】

【実施例】以下実施例につき本発明を詳細に説明する。

【００２５】図１は本発明の一実施例における暗号化装置としてのサーバと復号化装置としての携帯電話機を備えた通信システムの概要を表わしたものである。インターネット網２０１には各種データを格納したサーバ２０

２(図では１つのみを例示。）が接続されている。また、インターネット網２０１は携帯電話網２０３とも接続されている。携帯電話網２０３はエリアごとに基地局２０４(図では１つのみを例示。）と接続されている。基地局２０４は無線２０５によって情報通信端末の１つとしての携帯電話機２０６と接続されるようになっている。

【００２６】図２は、図１に示した暗号化装置としてのサーバの構成の概要を表わしたものである。サーバ２０２はＣＰＵ（中央処理装置）２２１を備えている。ＣＰＵ２２１はデータバス等のバス２２２を通じて各部と接続されている。このうち制御プログラム格納部２２３、解析ルール格納部２２４および送信データ格納部２２５は磁気ディスク（図示せず）の一部の記憶領域で構成できるもので、このうち制御プログラム格納部２２３にはサーバ２０２の各種機能を実現するための制御プログラムが格納されている。解析ルール格納部２２４は後に詳細に説明する暗号化するデータの分割や解析を行うためのルールが格納されている。送信データ格納部２２５は、送信する各種のデータを格納している。作業用メモリ２２６は、ＣＰＵ２２１の作業に伴って各種の手順やデータを一時的に格納するメモリであり、ランダム・アクセス・メモリ（ＲＡＭ）によって構成されている。通信制御部２２７は図１に示したインターネット網２０１と接続されており、データの送受信を行う回路装置である。

【００２７】なお、図１に示した携帯電話機２０６も図示しないがＣＰＵと、制御プログラムを格納したＲＯＭ（リード・オンリ・メモリ）および作業用メモリとしてのランダム・アクセス・メモリを備えている。そして、受信したデータを解読して元のデータに再現することができるようになっている。

【００２８】図３は、サーバの機能的な構成を示したものである。サーバ２０２は、図２に示した解析ルール格納部２２４に格納された解析ルール２４１を用いてデータの中身を解析してその結果に応じて複数のデータブロックに分割するデータブロック分割手段２４２と、分割されたそれぞれのデータブロックについての暗号の強度を決定する暗号強度決定手段２４３を備えている。暗号強度決定手段２４３は、データの重要度に応じて暗号の強度を決定する。この決定に基づいてデータブロック暗号化手段２４４はデータブロック単位で暗号化を行い暗号化データブロックを作成する手段である。暗号化データブロックはそれぞれ作業用メモリ２２６の所定の位置に格納されるようになっている。

【００２９】データブロック統合手段２４５は暗号化データブロックのそれぞれの暗号化方法と、暗号化データブロックの格納されている記憶領域の位置情報と、暗号化データブロックとを暗号化データとして統合する。このようにして統合された暗号化データが送信データとして図１に示した携帯電話機２０６に送出されることになる。以下、これを更に詳しく説明する。

【００３０】図４は本実施例で使用するルール情報としての重要部分を特定する情報の一覧を示したものである。図３に示した解析ルール２４１は、データをそれらの重要度に応じて分割するルールを表わした図４のようなルール情報２６１から構成されている。ルール情報２６１は、サーバ２０２から携帯電話機２０６に送信する暗号化データの元となる原データの種類ごとに用意されており、解析ルール格納部２２４に個別に格納されている。本実施例では原データの種類を大きく（１）構造化文書、（２）静止画像、映画等の動画像および（３）その他に分けて、これらの重要部分とそうでない一般部分を区分けしている。

【００３１】構造化文書では、タイトルおよび目次部分は重要度が低い一般部分と見なしている。これに対して本文については、重要度の高い重要部分と見なしている。たとえばWWW（world wide web）用の文書記述言語としてのＨＴＭＬ（Hyper Text Markup Language）文書では、図４に示したように「＜ｂｏｄｙ＞」タグの次から「＜／ｂｏｄｙ＞」タグに至るまでの文書部分を重要部分としている。この部分は本文としてその内容が表示されるからである。これ以外の文書部分は一般部分として重要度を低くしている。

【００３２】静止画像については、画像サイズ、ピクセルのサイズ、画像の圧縮方法などが記述されているヘッダ部分は画像を生成する上で重要であるので、重要部分と見なしている。これに対して、各ピクセルの画素の値を記載した箇所は重要度が低い一般部分と見なしている。具体的には図４に示したようにＧＩＦ（Graphics Interchange Format）４９ａフォーマットを例にとると、ＧＩＦストリームの開始を示「ＧＩＦ　Ｈｅａｄｅｒ」、「Ａｐｐｌｉｃａｔｉｏｎ　Ｅｘｔｅｎｓｉｏｎ」、「Ｇｒａｐｈｉｃ　Ｃｏｎｔｒｏｌ　Ｅｘｔｅｎｓｉｏｎ」、「Ｔｒａｉｌｅｒ」の部分を重要部分としている。これはこれらの部分はフォーマットならびに記載データが規定されており、一連のデータの中から特定することが可能である。これら以外の部分は一般部分として重要度を低くしている。

【００３３】これら以外にも、ｔｉｆｆ（Tag Image File Format）やｐｐｍ（Portable Pix Map)等のように各種の画像ファイルの形式は多数存在する。これらについてはフォーマットが規定されているので、これらを原データ内で特定して重要部分として処理する。これらのヘッダ部分以外は一般部分として重要度を低く設定する。

【００３４】ＪＰＥＧ（Joint Photographic Expert Group）およびＢＭＰ（Bit Map）ファイルについては、それぞれファイルの先頭から３０バイトおよび５４バイトがヘッダと規定されている。そこでこれらの部分を特定して重要部分とすることができる。これに対して米国ア

ップル社の「Ｑｕｉｃｋ　Ｔｉｍｅ」や、カラー動画像符号化方式としてのＭＰＥＧ（Moving Picture Experts Group）、動画と音声を交互に記録するＡＶＩ（Audio Video Interleaving）等の動画像については、最後の１０パーセントにクライマックスシーンが多い。そこで本実施例ではこれらについて原データの最後の１０パーセントの部分を重要部分とし、それら以外を一般部分としている。

【００３５】その他のファイルとしての以上説明した以外のファイル、たとえば実行可能を示す拡張子「ｅｘｅ」の存在する実行用ファイルについては、そのファイルの内部を解析することは困難である。このため、図４に示したように原データの先頭および末尾のＮバイトを重要部分とし、それら以外を一般部分と見なすことにしている。ここで数値Ｎは正の整数であるが、通常の場合、復号困難なバイト数を確保するという意味で数値Ｎは８（バイト）以上であることが好ましい。このようにデータの先頭および末尾を重要部分としたのは、コンピューターネットワークに不正にアクセスして、データを改ざんしたり破壊する等の行為を行うクラッカがデータを復号するにあたって、対象となるデータの先頭あるいは末尾の部分から作業を開始する可能性が高いからである。

【００３６】図４に示した重要部分を特定するルールは原データが解析可能な場合を中心とした解析ルールである。これ以外にも、バイナリデータからそのまま重要部分とそれ以外の一般部分の識別を行うことも可能である。たとえば原データのうちの同じ値が連続する部分は解読されてもクラッカがそのデータを復元しにくい。そこでこのような部分を一般部分とし、それ以外の部分を重要部分とすることができる。このように図４に示した解析ルール格納部２２４は種々の定義を行うことができる。このため、図４に示した重要部分を特定するルールは、原データの性質に応じて各種の設定が可能であり、図４に示すものに限定されるものではない。

【００３７】データブロック分割手段２４２は、図４に示した重要部分を特定するルールに基づいてサーバ２０２からクライアントとしての携帯電話機２０６に送信する原データの内容を解析して、重要度別となったデータブロックに区分けあるいは分割する。

【００３８】図５は、このデータブロック分割処理の流れを表わしたものである。図２に示したＣＰＵ２２１は拡張子あるいはファイルの先頭に存在する識別子を基にして、処理の対象となる原データが構造化文書であるかどうかを判別する（ステップＳ３０１）。ＨＴＭＬ文書に代表される構造化文書であれば（Ｙ）、そのタグを解析する（ステップＳ３０２）。そして、これにより重要度別にデータブロックを分割する（ステップＳ３０３）。

【００３９】一方、同様にしてＣＰＵ２２１が原データを静止画であると判別したときには（ステップＳ３０４：Ｙ）、ヘッダの解析を行って（ステップＳ３０５）、重要度別にデータブロックを分割する（ステップＳ３０３）。

【００４０】以上と異なり原データが動画像であると判別したときには（ステップＳ３０６：Ｙ）、フレームの解析を行って（ステップＳ３０７）、重要度別にデータブロックを分割する（ステップＳ３０３）。

【００４１】原データが以上のいずれにも該当しない場合には（ステップＳ３０６：Ｎ）、その先頭と末尾の解析を行う（ステップＳ３０８）。そして、図４で示した内容に従って重要度別にデータブロックを分割する（ステップＳ３０３）。ステップＳ３０３の処理が終了したら、その結果を暗号強度決定手段２４３に出力して（ステップＳ３０９）、データブロック分割処理が終了する（エンド）。

【００４２】図６は暗号強度決定手段の処理の流れを表わしたものである。暗号強度決定手段２４３はデータブロックを１ブロック分読み込み（ステップＳ３２１）、そのデータブロックの重要度に応じて暗号アルゴリズムと暗号鍵の長さを決定する（ステップＳ３２２）。図４ではデータブロックの重要度を重要部分のとそれ以外の一般部分の２つに分類しているので、データブロック分割手段２４２で分割されたデータブロックのそれぞれを前記した２つの重要度のいずれかに分類することができる。

【００４３】決定された暗号強度が強いほど、暗号としての強度の強いアルゴリズムや長い暗号鍵の選択が行われる。したがって、前記したテーブルは暗号アルゴリズムや暗号鍵の長さを対応付けておくことでそれぞれのデータブロックから暗号アルゴリズムや暗号鍵の長さの決定を簡単に行うことができる。

【００４４】このようにして暗号アルゴリズムと暗号鍵の長さが決定されたら、後続のデータブロックが存在しているかどうかをチェックして（ステップＳ３２３）、存在していれば（Ｙ）、ステップＳ３２１に戻ってその処理を開始する。すべてのデータブロックの処理が終了したら（ステップＳ３２３：Ｎ）、それぞれの結果をデータブロック暗号化手段２４４に出力して（ステップＳ３２４）、暗号強度決定手段２４３による処理が終了する（エンド）。なお、暗号強度決定手段２４３はデータブロックの処理が１つずつ終了するたびにこれらの結果を逐次データブロック暗号化手段２４４に出力してもよい。

【００４５】図７は、データブロック暗号化手段の処理の流れを表わしたものである。データブロック暗号化手段２４４はデータブロックを１ブロック分読み込み（ステップＳ３４１）、指示された暗号アルゴリズムおよび暗号鍵の長さからなる暗号化方法でそのデータブロックを暗号化する（ステップＳ３４２）。

【００４６】このようにして暗号化データが生成されたら、後続のデータブロックが存在しているかどうかをチェックして（ステップＳ３４３）、存在していれば（Ｙ）、ステップＳ３４１に戻ってその処理を開始する。すべてのデータブロックの処理が終了したら（ステップＳ３４３：Ｎ）、これら暗号化ブロックとこれらに対応する暗号化方法とを組にしてデータブロック統合手段２４５に出力して（ステップＳ３４４）、データブロック暗号化手段２４４による処理が終了する（エンド）。

【００４７】データブロック統合手段２４５は、データブロック暗号化手段２４４から出力された暗号化データブロックと、各データブロックにおける暗号化方法およびデータ位置情報が記憶されている暗号化情報ブロックを統合する。そして暗号化データとして出力することになる。ここでデータ位置情報とは、暗号化データブロックの位置を特定するための先頭および末尾のアドレスあるいは先頭のアドレスおよびデータ長からなる情報である。このデータブロック統合手段２４５の統合の手法は２通り存在する。

【００４８】図８は第１の手法で統合された暗号化データの構成を示したものである。第１の手法で統合された暗号化データ４０１の先頭には、統合された暗号化情報ブロック４０２が１つ配置されており、これに続いてそれぞれの暗号化データブロック４０３_1、４０３_2、……４０３_mが配置されている。このような暗号化データ４０１では、暗号化情報ブロック４０２が先頭に総合された形で配置されているので、復号の処理が簡単になるという長所がある。

【００４９】この暗号化情報ブロック４０２は必ずしも暗号化データ４０１の先頭に配置する必要はない。すなわち、暗号化情報ブロック４０２を識別可能にするための特別のフラグを配置したり、あるいは暗号化データ４０１の先頭に暗号化情報ブロック４０２の先頭のアドレスを記載しておく等の手法を採ることで任意の位置に配置することが可能になる。

【００５０】暗号化情報ブロック４０２内には、それぞれの暗号化データブロック４０３_1、４０３_2、……４０３_mについての暗号化方法とこれらの先頭アドレスおよび末尾アドレスが格納されている。先頭アドレスはデータの先頭あるいは暗号化データブロック４０３の終端からのバイト数あるいはビット数で表わされる。末尾アドレスを格納する代わりに、先頭アドレスから末尾アドレスまでのデータ長を格納してもよい。また、クライアントとしての携帯電話機２０６側に事前に復号鍵を送付していないような場合には、復号鍵もこの暗号化情報ブロック４０２内に格納することができる。

【００５１】図９は第２の手法で統合された暗号化データの構成を示したものである。第２の手法で統合された暗号化データ４１１は、それぞれの暗号化データブロック４０３_1、４０３_2、……４０３_mの直前に個別に暗号化情報ブロック４１２_1、４１２_2、……４１２_mを配置している。ただし、それぞれの暗号化データブロック４０３_1、４０３_2、……４０３_mの開始位置を第三者が解読しにくいようにするためには、特開平０７－２８１５９６号公報にも開示されているように暗号化情報ブロック４１２と暗号化データブロック４０３の間に乱数を挿入することも有効である。

【００５２】この図９に示した手法では、それぞれの暗号化情報ブロック４１２_1、４１２_2、……４１２_mに、暗号化データブロック４０３_1、４０３_2、……４０３_mのうちの対応するものの暗号化情報およびデータ長を格納することになる。暗号化情報ブロック４１２_1、４１２_2、……４１２_mのデータ長が可変であったり、暗号化情報ブロック４１２_1、４１２_2、……４１２_mと暗号化データブロック４０３_1、４０３_2、……４０３_mのうちの対応するものとの間に何らかのダミーデータが挿入されているような場合がある。このような場合には、先頭アドレスあるいは末尾アドレスのいずれかをデータ長に加えたり、あるいはデータ長自体は記録せずに先頭アドレスと末尾アドレスの双方を記録するようにすればよい。この第２の手法でも、第１の手法と同様に、携帯電話機２０６側に事前に復号鍵を送付していないような場合では、暗号化情報ブロック４０２内に復号鍵を格納することができる。

【００５３】以上の第１の手法と第２の手法いずれの場合でも、暗号化情報ブロック４０２、４１２_1、４１２_2、……４１２_mとして暗号化していないデータを使用することもできるし、セキュリティを高めるためにサーバ２０２と携帯電話機２０６の間で事前に取り決めた暗号アルゴリズムで暗号化したデータを使用することもできる。

【００５４】図１０は携帯電話機側の復号化装置の構成の概要を表わしたものである。図１に示したクライアントとしての携帯電話機２０６は、インターネット網２０１、携帯電話網２０３および基地局２０４を介して受信した暗号化データ４０１（４１１）からデータブロックを分割するデータブロック分割手段５０１を備えている。データブロック分割手段５０１で分割された個々のデータブロックは、データブロック復号手段５０２で復号化され、データ統合手段５０３によって原データに統合されるようになっている。

【００５５】なお、データブロック分割手段５０１、データブロック復号手段５０２およびデータ統合手段５０３は、サーバ２０２側の図３で示した各手段と同様に図示しないＣＰＵとこれが実行するプログラムによって機能的に実現する手段である。もちろん、これらの一部または全部をハードウェアで実現することも可能である。

【００５６】図１１はデータブロック分割手段の処理の流れを表わしたものである。携帯電話機２０６は暗号化

データ４０１（４１１）を受信すると（ステップＳ５２１：Ｙ）、暗号化情報ブロックが暗号化されているかどうかを事前の取り決め内容等によって判別する（ステップＳ５２２）。暗号化されている場合には（Ｙ）、図８または図９に示した暗号化情報ブロック４０２（412_1、412_2、……412_m）を復号化する（ステップＳ５２３）。そして、暗号化情報ブロック４０２（412_1、412_2、……412_m）の内容に基づいて、暗号化データを元の複数の暗号化データブロック403_1、403_2、……403_m（図８、図９参照）に分割する（ステップＳ５２４）。暗号化情報ブロック４０２（412_1、412_2、……412_m）を暗号化していない場合には（ステップＳ５２２：Ｎ）、直ちにステップＳ５２４の処理が行われる。ステップＳ５２４の処理が終了したら、暗号化データブロック403_1、403_2、……403_mをデータブロック復号手段５０２に出力して（ステップＳ５２５）、データブロック分割手段５０１の処理を終了させる（エンド）。

【００５７】図１２は、データブロック復号手段の処理の流れを表わしたものである。データブロック復号手段５０２は、データブロック分割手段５０１から入力された暗号化データブロック403_1、403_2、……403_mに暗号鍵が添付されているかどうかを判別し（ステップＳ５４１）、添付されている場合にはその暗号鍵を使用して暗号化データブロック403_1、403_2、……403_mを復号する（ステップＳ５４２）。このとき、暗号化情報ブロック４０２（412_1、412_2、……412_m）に格納されている対応する暗号化方法に基づいてこれらの暗号化データブロック403_1、403_2、……403_mを復号することになる。特開平２０００－４７５８０号公報に開示されているように、暗号鍵を所定の方法（たとえばＰＫＩあるいはＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ法）で事前に交換している場合には、（ステップＳ５４１：Ｎ）、事前に得られたその暗号鍵を使用し、暗号化情報ブロック４０２（412_1、412_2、……412_m）に格納されている対応する暗号化方法に基づいてこれらの暗号化データブロック403_1、403_2、……403_mを復号する（ステップＳ５４３）。

【００５８】ステップＳ５４２あるいはステップＳ５４３の処理がすべての暗号化データブロック403_1、403_2、……403_mについて終了したら、データブロック復号手段５０２は復号された各データをデータ統合手段５０３に出力することになる（ステップＳ５４４）。

【００５９】図１３は、データ統合手段の処理の流れを表わしたものである。データ統合手段５０３は各ブロックごとのデータを１つずつ統合し（ステップＳ５６１）、統合するデータが存在する間はこの手順を繰り返す（ステップＳ５６２：Ｎ）。すべてのデータの統合が終了したら（Ｙ）、これによって復元された原データを、携帯電話機２０６（図１）の文字や映像等の情報再生用の領域あるいは回路装置（図示せず）に出力することになる（ステップＳ５６３）。

【００６０】以上説明した実施例ではデータブロック分割手段２４２が２種類のデータブロックに分割し、このうちの重要部分のデータブロックには暗号強度の強い暗号化手法を採用し、これ以外の一般部分のデータブロックについては暗号強度の弱い暗号化手法を採用した。これにより従来と比べると重要部分のセキュリティを充分向上させることができる。もちろん、図４に示したルール情報を複数の重要度に区分けしておけば暗号化強度を多段階に設定することができる。

【００６１】発明の第１の変形例

【００６２】図１４は、本発明の第１の変形例におけるサーバの構成の概要を表わしたものである。この図１４で先の実施例の図３と同一部分には同一の符号を付しており、これらの説明を適宜省略する。第１の変形例のサーバ２０２Ａのデータブロック分割手段２４２は、解析ルール格納部２２４に格納された解析ルール２４１を用いてデータの中身を解析し、原データを複数のデータブロックに分割してブロック長検出手段６０１に出力するようになっている。ブロック長検出手段６０１はこれらのデータブロック長を検出し、暗号強度決定手段２４３Ａは検出されたデータブロック長に応じて暗号化の強度を調整する。

【００６３】たとえば、データブロック長の短いものについては暗号アルゴリズムが弱いと簡単にデータを復元されてしまう危険性がある。そこで、このようなものについては暗号の標準方式の１つとしてのＴｒｉｐｌｅ ＤＥＳ（Triple Data Encryption Standard）のように比較的暗号強度の強いものを選択する。また、中程度のデータブロック長の場合にはＤＥＳ（Data Encryption Standard）のような中程度の暗号化強度を選択する。データブロック長の長いものの場合にはＤＥＳの撹乱回数を少数にしたもののように暗号強度の比較的弱いものを選択する。このような暗号化強度のきめ細かな選択によって、データブロック暗号化手段２４４はそれぞれのデータブロックに応じた適切な暗号化を行うことができる。

【００６４】これにより、データのセキュリティを比較的高く保ちながら、携帯電話機２０６側では暗号強度の比較的弱いものについては復号に際する負担を軽減することができ、全体としての復号に要する時間を従来よりも短縮することができる。

【００６５】発明の第２の変形例

【００６６】図１５は、本発明の第２の変形例におけるサーバの構成の概要を表わしたものである。この図１５で第１の変形例の図１４と同一部分には同一の符号を付しており、これらの説明を適宜省略する。第２の変形例のサーバ２０２Ｂは、第１の変形例のサーバ２０２Ａと同様にデータブロック長の検出を行うブロック長検出手

段６０１を備えている。このブロック長検出手段６０１の検出結果は復号予定時間検出手段６２１に入力されるようになっている。

【００６７】図１６は復号予定時間検出手段の処理の流れを表わしたものである。復号予定時間検出手段６２１は原データの種類に応じて復号予定時間の検出を行う。原データが動画の場合には（ステップＳ６４１：Ｙ）、３３ｍｓｅｃ（ミリ秒）に設定する（ステップＳ６４２）。アニメーションＧＩＦ（Graphics Interchange Format）の場合には（ステップＳ６４３：Ｙ）、データの内部に記載されている表示間隔によって復号予定時間を規定する（ステップＳ６４４）。これ以外の場合、すなわち原データが静止画やテキスト情報の場合には（ステップＳ６４３：Ｎ）、デコード時間に違和感が無い程度の時間として一例として復号予定時間を３秒に設定する（ステップＳ６４５）。このようにして復号予定時間が検出されたらこれを暗号強度決定手段２４３Ｂに出力する（ステップＳ６４６）。本実施例の暗号強度決定手段２４３Ｂは図１５に示すように復号速度データ格納部６２２から復号速度データ６２３の供給も受けるようになっている。

【００６８】図１５に戻って説明を続ける。暗号強度決定手段２４３Ｂでは、復号速度データ格納部６２２から供給された復号速度データ６２３に基づいて各データブロックの暗号強度を調整する。復号速度データ６２３は、クライアントとしての携帯電話機２０６でサポートしている暗号化方法のすべてについてデコード速度Ｖｉ（バイト／ｓｅｃ）を事前に測定して得られたデータであり、復号速度データ格納部６２２に格納されている。ここで符号ｉは、暗号化方法を特定するためのインデックスを示している。

【００６９】暗号強度決定手段２４３Ｂは、復号予定時間をＴ（ｓｅｃ）、また各データブロック長をＬｊとしたとき、次の（１）式を満足するように各データブロックの暗号化方法を決定する。ここで符号ｊは、暗号化方法を特定するためのインデックスを示している。

【００７０】

【数１】

$$T = \sum_{i} \frac{L_j}{V_i} \qquad \cdots\cdots (1)$$

【００７１】暗号化方法の決定については、各データブロックの重要度を拘束条件とした線形計画法を使用して最適な暗号化手法を計算することが可能である。しかしながら、このような手法に限定されるものではなく、重要部分で暗号強度が強く、その他の一般部分で暗号強度が弱くなっていれば、他の手法も利用可能である。このようにして決定された各データブロックの暗号化方法は解析データ記憶手段６２４に順次格納される。

【００７２】データブロック暗号化手段２４４Ａは、解析データ記憶手段６２４に格納されている暗号化方法でそれぞれ対応するデータブロックの暗号化を行う。データブロック統合手段２４５は暗号化されたデータブロックと各データブロックにおける暗号化方法およびデータ位置情報が記憶されている暗号化情報ブロックを統合する。そしてこれを暗号化データとして出力することになる。

【００７３】この第２の変形例によれば、クライアントでサポートしている全暗号化方法のデコード速度を予め測定しておき、データブロックに応じて暗号化方法を適応的に選択している。このため、復号予定時間に合わせて復号化データを作成することが可能になる。

【００７４】なお、実施例および変形例では携帯電話機を例に挙げて説明したが、本発明の暗号化および復号化の適用される装置はこれに限られるものではなく、ＰＨＳ（Personal Handyphone System）、ＰＤＡその他の情報通信端末を含むものであることは当然である。

【００７５】

【発明の効果】以上説明したように請求項１～請求項４記載の発明によれば、送信すべき原データを構成する各部分の重要度に応じて暗号化の強度を選択することにしたので、例えば一部のみ重要なデータについてはその部分のみ暗号化の強度を高めればよく、復号化の際の処理を全体的に迅速に行わせることができるという効果がある。

【００７６】また請求項２～請求項４記載の発明によれば、送信すべき原データを構成する各部のデータの種類を判別して、暗号化の強度をこれに応じて定めているので、処理が画一的で簡単になるという利点がある。

【００７７】更に請求項３記載の発明では、ブロック長判別手段によって判別されたブロック長を勘案して暗号化の強度の重要度を判別するので、よりきめ細かな暗号化を行うことができ、復号の際の処理の負担を軽減させることができる。

【００７８】また請求項４記載の発明によれば、分割されたデータブロックの種類ごとに復号が行われる側での復号の予定時間を検出し、検出された時間に合わせてデータの種類も考慮しながら暗号化の強度を選択するようにしているので、暗号化されたデータを復号する装置側の負荷等を考慮しながら合理的な暗号化を行うことができ、復号の際の処理の負担を軽減させることができる。

【００７９】更に請求項５記載の発明によれば、暗号化されたデータを受信してこれをデータの種類別のデータブロックに分割し、それぞれのデータブロックごとの暗号化方法を示すデータを基にしてデータブロック単位に復号するので、重要度の低いデータブロックについての処理が大幅に軽減され、全体的な処理の負担を軽減したり、処理の速度を向上させることができる。

【００８０】また請求項６記載の発明によれば、予め取得した暗号鍵を使用してデータブロックごとの暗号化方法を復号し、これを用いて対応するデータブロックの復

号を行うので、データのセキュリティを充分確保することができる。

【図面の簡単な説明】

【図１】本発明の一実施例における暗号化装置としてのサーバと復号化装置としての携帯電話機を備えた通信システムの概要を表わしたシステム構成図である。

【図２】図１に示した暗号化装置としてのサーバの構成の要部を表わしたブロック図である。

【図３】本実施例のサーバの機能的な構成を示したブロック図である。

【図４】本実施例で使用するルール情報としての重要部分を特定する情報の一覧を示した説明図である。

【図５】本実施例のデータブロック分割処理を表わした流れ図である。

【図６】本実施例の暗号強度決定手段の処理を表わした流れ図である。

【図７】本実施例のデータブロック暗号化手段の処理を表わした流れ図である。

【図８】本実施例で第１の手法で統合された暗号化データの構成を示した説明図である。

【図９】本実施例で第２の手法で統合された暗号化データの構成を示した説明図である。

【図１０】本実施例でクライアントとしての携帯電話機側の復号化装置の構成の概要を表わしたブロック図である。

【図１１】本実施例でデータブロック分割手段の処理を表わした流れ図である。

【図１２】本実施例でデータブロック復号手段の処理を表わした流れ図である。

【図１３】本実施例でデータ統合手段の処理を表わした流れ図である。

【図１４】本発明の第１の変形例における暗号化装置としてのサーバの構成の要部を表わしたブロック図である。

【図１５】本発明の第２の変形例における暗号化装置としてのサーバの構成の要部を表わしたブロック図である。

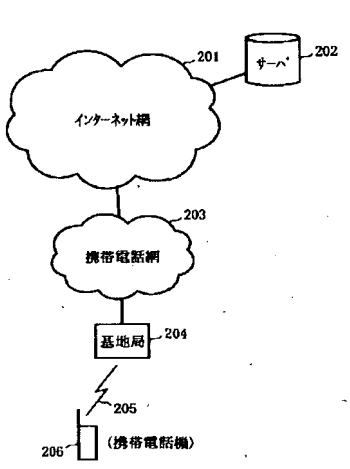
【図１６】第２の変形例における復号予定時間検出手段の処理の流れを表わした流れ図である。

【図１７】暗号化されたデータの復号化を簡略化することのできる第１の提案の概要を示した説明図である。

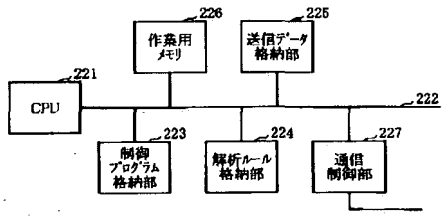
【符号の説明】

２０１　インターネット網
２０２、２０２Ａ、２０２Ｂ　サーバ
２０６　携帯電話機（情報通信端末）
２２１　ＣＰＵ（中央処理装置）
２２３　制御プログラム格納部
２２４　解析ルール格納部
２４１　解析ルール
２４２　データ分割手段
２４３、２４３Ａ、２４３Ｂ　暗号強度決定手段
２４４、２４４Ａ　データブロック暗号化手段
２４５　データブロック統合手段
４０１、４１１　暗号化データ
４０２、４１２　暗号化情報ブロック
４０３　暗号化データブロック
５０１　データブロック分割手段
５０２　データブロック復号手段
５０３　データ統合手段
６０１　ブロック長検出手段
６２１　復号予定時間検出手段
６２２　復号速度データ格納部
６２４　解析データ記憶手段

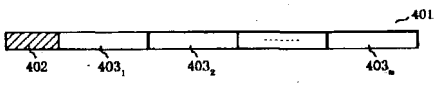
【図１】



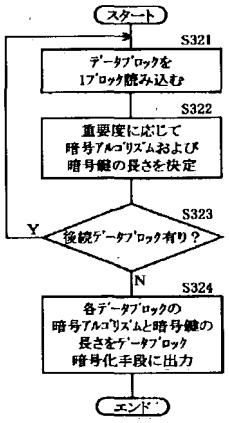
【図２】



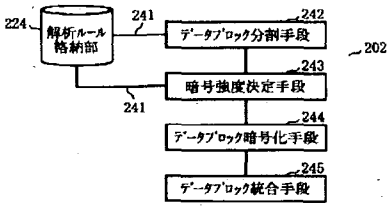
【図８】



【図６】



【図３】

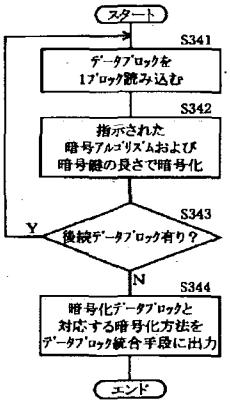


【図４】

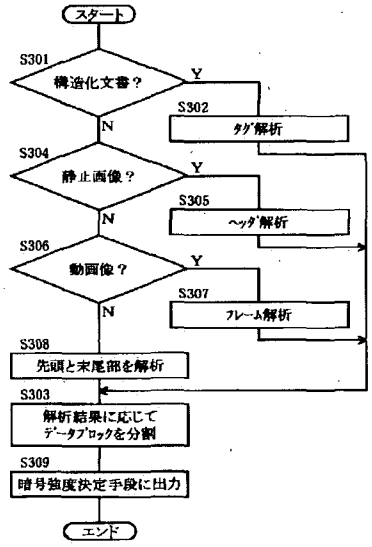
261

データ種類	重要部分
HTML	<body></body>
⋮	⋮
GIF 94a	GIF Header, Application Extension, Graphic Control Extension, Trailer
JPEG	先頭から30byte
BMP	先頭から54byte
⋮	⋮
Quick Time, MPEG, AVIなど	データの最後の10%
その他	データの先頭と末尾のN byte

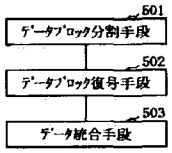
【図７】



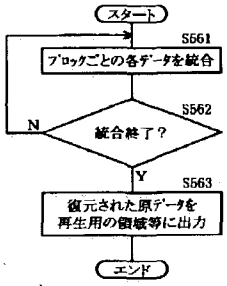
【図５】



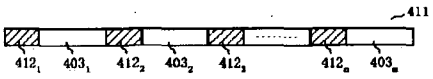
【図１０】



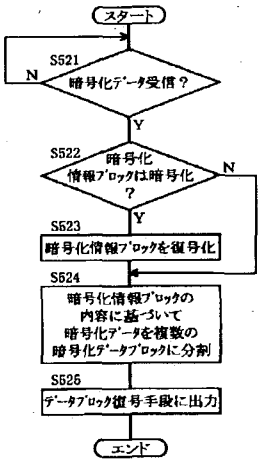
【図１３】



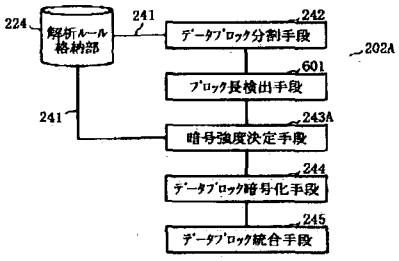
【図９】



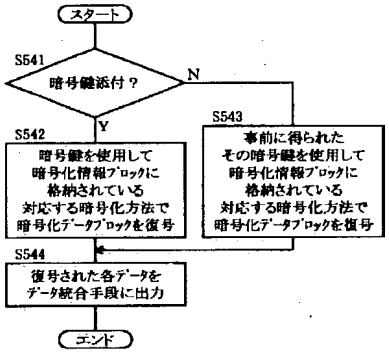
【図１１】



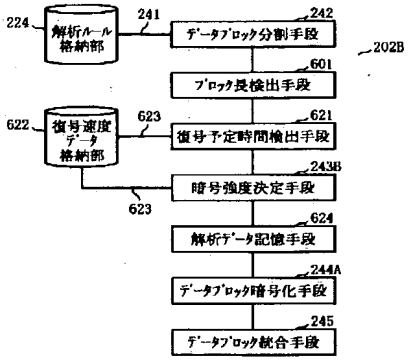
【図１４】



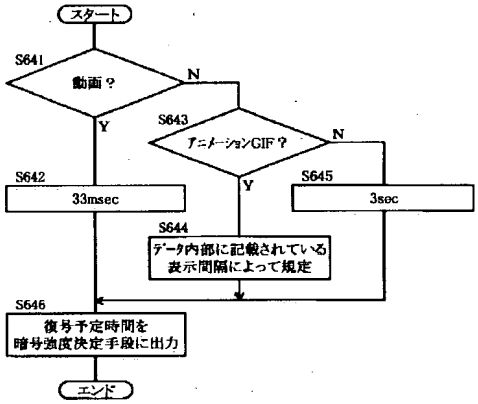
【図１２】



【図１５】



【図１６】



【図１７】